IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

JAMES W. FAHRNY et al.

Serial No.: 10/767,980

Filed: January 29, 2004

For: System and Method for Security Processing Media Streams

Attorney Docket No.: 2004008014 (CCCI0128PUS)

Group Art Unit: 2135

Examiner: Thomas A. Gyorfi

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Mail Stop Appeal Brief - Patents
Commissioner for Patents
U.S. Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an Appeal Brief from the final rejection of claims 1-28 of the Office Action mailed on August 2, 2007, for the above-identified patent application.

I. REAL PARTY IN INTEREST

The real party in interest is Comcast Cable Holdings, LLC ("Assignee"), a corporation organized and existing under the laws of the state of Delaware, and having a place of business at 1500 Market Street, 34th Floor, Philadelphia, Pennsylvania, 19102, as set forth in the assignment recorded in the U.S. Patent and Trademark Office on June 23, 2004, at Reel 014775/Frame 0153.

II. RELATED APPEALS AND INTERFERENCES

There are no appeals or interferences known to the Appellant, the Appellant's legal representative, or the Assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1-28 are pending in this application. Claims 1-28 have been rejected and are the subject of this appeal.

IV. STATUS OF AMENDMENTS

No amendments to the claims were filed after final rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER

As illustrated in Figures 1-3, claim 1 provides a system (200) for multi-stream security processing and distributing digital media streams. The system includes a headend (202) configured to generate encrypted digital media streams and download software. A network (204) is coupled to the headend and is configured to receive the encrypted digital media streams and downloaded software. At least one receiver (100, 206a ... 206n, 208a ... 208n) is coupled to the network and is configured to receive the encrypted digital media streams (110) and downloaded software (*e.g.*, 116) and to present a decrypted version of the encrypted digital media streams (112) based on the downloaded software. The receiver comprises a security processor (102, 212a ... 212n) configured to provide at least one of simultaneous multiple encryption and simultaneous multiple decryption processing of the digital media streams, the security processor operative to store the downloaded software and to securely configure, renew, and re-configure at least one of encryption and decryption by the security processor based on the downloaded software.

Similarly, independent claim 11 provides a method of multi-stream security processing and distributing digital media streams. Encrypted digital media streams are generated at a headend (202). A network (204) is coupled to the headend and receives the encrypted digital media streams at the network. A receiver (100, 206a ... 206n, 208a ... 208n) is coupled to the network and receives a software download (*e.g.*, 116) from the network. The encrypted digital media streams (110) are received at the receiver. A decrypted version of the encrypted digital media streams (112) is presented using the receiver. A security processor

(102, 212a ... 212n) in the receiver is reconfigured based on the software download to provide at least one of simultaneous multiple encryption and simultaneous multiple decryption processing of the digital media streams. The software download is stored in the security processor (*e.g.*, 104, 106, 136).

Similarly, independent claim 20 provides a security processor (102, 212a ... 212n) for use in a system for multi-stream security processing and distributing digital media streams. The security processor is configured to provide at least one of simultaneous multiple media stream decryption and encryption processing. The security processor includes a controller (132) operative to be programmed through authenticated firmware downloads from a headend, each firmware download operative to modify media stream processing by the security processor. A memory (*e.g.*, 104, 106, 136) stores the downloaded firmware. A plurality of digital stream encryption/decryption engines (130, 140a ... 140n) are selectively coupled by the controller for simultaneous operation in response to a predetermined security configuration downloaded to the controller.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-28 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,424,717 to Pinder *et al.* (henceforth, "Pinder") in view of U.S. Patent No. 5,784,095 to Robbins *et al.* (henceforth, "Robbins").

VII. ARGUMENT

Appellants respectfully ask the Board to overturn the Examiner's rejections in light of the following arguments.

A. Claims 1-28 Are Patentable Under 35 U.S.C. § 103(a) <u>Over Pinder In View Of Robbins</u>

1. Claims 1 And 11 Are Patentable <u>Over Pinder In View Of Robbins</u>

Claim 1 provides a system for multi-stream security processing and distributing digital media streams. The system includes a headend, a network coupled to the headend, and at least one receiver coupled to the network. The headend is configured to generate encrypted digital media streams and download software. The receiver is configured to receive the encrypted digital media streams and downloaded software and to present a decrypted version of the encrypted digital media streams based on the downloaded software. The receiver includes a security processor configured to provide at least one of simultaneous multiple encryption and simultaneous multiple decryption processing of the digital media streams. The security processor stores the downloaded software and securely configures, renews, and re-configures at least one of encryption and decryption by the security processor based on the downloaded software.

Independent claim 11 provides a method of multi-stream security processing and distributing digital media streams. Encrypted digital media streams are generated at a headend. A network is coupled to the headend and receives the encrypted digital media streams. A receiver is coupled to the network, the receiver receiving a software download from the network. The encrypted digital media streams are received at the receiver. A decrypted version of the encrypted digital media streams is presented using the receiver. A security processor in the receiver is re-configured based on the software download to provide at least one of simultaneous multiple encryption and simultaneous multiple decryption processing of the digital media streams. The software download is stored in the security processor.

In the final Office Action, the Examiner rejected claims 1 and 11 as an obvious combination of Pinder and Robbins using the same argument. However, neither Pinder nor Robbins teach or fairly suggest software downloaded to a security processor from a headend

that configures or reconfigures the security processor for encryption or decryption of digital media streams.

The Examiner admitted that Pinder does not disclose Appellants' security processor reconfigured by downloaded software as claimed. (Final Office Action, pg. 3.) Instead, the Examiner offered Robbins, stating as the only support "col. 5, lines 1-6, col. 13, lines 65-67." (Office Action, pg. 3.) The paragraph including the first cited passage is provided below.

> The CDC 34 is used to control the settop terminal 112 through commands that initialize and configure the settop terminal 112. The settop terminal 112 incorporates a microprocessor executing a program loaded into an EEPROM (as firmware) for the various levels of services. The CDC 34 can be used to download new releases of settop terminal 112 firmware from the headend 16 when system 10 requirements change or new features are desired. The CDC 34 will service the settop terminal 112 and all of its options. In the preferred embodiment, the control data is sent at a rate of 13,980 bits per second.

Robbins discloses downloading software to implement new "services" or "features." There is no mention of downloading software which <u>configures or reconfigures</u> a security processor for encrypting or decrypting digital media streams.

The second cited passage likewise makes no mention of downloading software which <u>configures or reconfigures</u> a security processor for encrypting or decrypting digital media streams.

> The system microprocessor 329 interprets all commands from either the interface keys 323, the navigation keys 325, the remote commander 333, or an IR emitter and responds accordingly. The system microprocessor 329 also receives settop terminal control and channel mapping information broadcast from the system headend 16 by using the CDC 34 from the tuner FM receiver tap 341. This separate control channel updates the system firmware stored in ROM 337 with new releases whenever user subscriptions change or for security. Additionally, program schedule information is periodically

> downloaded from the system headend 16 to individual subscribers.

Updating firmware for subscription changes or for security purposes does not teach, or fairly suggest, configuring or reconfiguring a processor for encrypting or decrypting digital media streams.

In response, the Examiner provided the following argument.

> Examiner disagrees. Note that the passage(s) from Robbins state that the firmware can configure the box to update what services a user is subscribed to; such changes would necessarily involve adding a subscription to a channel (i.e. being able to decrypt a channel/stream that one could not previously decrypt) or unsubscribing (no longer being able to decrypt a channel/stream that one could previously able to). These conditions satisfy both the claim language and Applicant's argued limitation.

(Advisory Action, pg. 2.)

The Examiner's argument is based on layers of supposition. The Examiner first assumes that "adding a subscription to a channel" or "unsubscribing" inherently discloses modifying the decryption process in some manner. Clearly this is not the case. A wide variety of changes can be made to cable services without any change to the decryption process provided by the settop box. The Examiner also inaccurately equates changing subscription parameters with Appellants' downloading software that configures encryption or decryption by a security processor.

In addition to failing to find disclosure in either Pinder or Robbins for software downloaded to a security processor from a headend that configures or reconfigures the security processor for encryption or decryption of digital media streams, Pinder, the Examiner's primary reference, actively teaches away from the combination suggested by the Examiner. Pinder discloses encryption and decryption code which is unalterably locked into ROM at the time in which the Digital Home Communication Terminal Secure Element (DHCTSE) is manufactured.

> Memory 1207 contains the code executed by microprocessor 1201, the keys, and the entitlement information.

> In a preferred embodiment, there are **two kinds of physical memory in memory 1207: ROM 1219, which is read-only memory whose contents are fixed when DHCTSE 627 is manufactured**, and non-volatile memory (NVM) 1209, which can be read and written like normal random-access memory, but which retains its current values when DHCTSE 627 is without power.
>
> * * *
>
> FIG. 13 is a schematic **overview of the contents of memory 1207 in DHCTSE 627. The memory is divided into two main parts: read-only storage 1301, which contains code and other information that does not change as a result of the interpretation of EMMs**, and NVA storage 1303, which is non-volatile storage that changes as a result of the interpretations of EMMs. **RO storage 1301 contains code 1305**.
>
> **Code 1305 falls into four categories: code 1307 for the encryption, decryption, and authentication operations** performed by DHCTSE 627, code for interpreting EMMs 1313, code for interpreting ECMs 1321, and code for handling other CA messages such as the FPM and the GBAM.
>
> (Pinder, col. 21, ln. 49-col. 22, ln. 12 (emphasis added).)

In response to this argument, the Examiner provided the following rebuttal in the Advisory Action:

> With respect to Applicant's argument that Pinder teaches away from the combination of references, it is observed that while the encryption algorithms may be hardcoded into the Pinder device, the claim language is broadly written in such a way as to merely recite that the ability of the terminal to either encrypt or decrypt content - and not necessarily the actual encryption algorithm itself, as per Applicant's narrow interpretation of the claim language - is what is materially affected by a software update. Pinder clearly discloses wherein that device is capable of updating entitlement information which, when granted permits a user to view encrypted content that one could not previously decrypt, and vice versa (see col. 29 as an example); this clearly conforms to the "configure, renew, and re-configure" the ability to encrypt or decrypt streams, as recited for example by claim 1. Additionally, since Robbins discloses wherein such an update to alter the ability to encryp/decrypt content is part and parcel of a software/firmware update, the

> claim thus remains obvious over the combination of references as discussed in the previous Office Action.
>
> (Advisory Action, pg. 2.)

The Examiner first admits that "the encryption algorithms may be hardcoded into the Pinder device." The Examiner then argues that the claims only require encryption and decryption, "and not necessarily the actual encryption algorithm itself." Claim 1 provides for a "receiver ... configured to receive the encrypted digital media streams and downloaded software and to present a decrypted version of the encrypted digital media streams based on the downloaded software." The decryption is accomplished by the downloaded software. Moreover, claim 1 further provides a "security processor operative to store the downloaded software and to securely configure, renew, and re-configure at least one of encryption and decryption by the security processor based on the downloaded software." It is the encryption or decryption process which is reconfigured by the downloaded software. Claim 11 similarly provides for "re-configuring a security processor in the receiver based on the software download to provide at least one of simultaneous multiple encryption and simultaneous multiple decryption processing of the digital media streams."

The Examiner's final argument is that "Pinder clearly discloses wherein that device is capable of updating entitlement information which, when granted permits a user to view encrypted content that one could not previously decrypt, and vice versa (see col. 29 as an example)." The column referenced by the Examiner deals with entitlement management messages. Such subscriber entitlements do not disclose or remotely suggest Appellants' downloaded software for encryption or decryption.

> The authorization information used in a particular set top box 113(i) is obtained from one or more entitlement management messages 111 addressed to set top box 113(i). Subscribers generally purchase services by the month (though a service may be a one-time event), and after a subscriber has purchased a service, service distribution organization 103 sends set top box 113(i) belonging to the subscriber entitlement management messages 111 as required to provide the authorization information 121 required for the purchased services.

(Pinder, col. 4, ll. 52-61.)

Entitlement management messages (EMMs), and authorization in general, specify what services may be accessed by a subscriber. Pinder's disclosure of EMMs certainly does not contradict, or even weaken, Pinder's express rejection of Appellants' invention. In fact, Pinder discloses that both the decryption logic and the logic for handling EMMs is stored in "read-only storage ... which contains code and other information that does not change as a result of the interpretation of EMMs." (Pinder, col. 22, ll. 3-5. See full quote above.)

Neither Pinder nor Robbins, alone or in combination, teaches or fairly suggests Appellants' security processor that is configured or reconfigured from software downloaded to the security processor to provide encryption or decryption processing of digital media streams. Claims 1 and 11 are patentable over Pinder and Robbins. Claims 2-10 and 12-19, which depend from claims 1 and 11, respectively, are therefore also patentable.

2. **Claim 20 Is Patentable Over <u>Pinder In View Of Robbins</u>**

Independent claim 20 provides a security processor configured to provide at least one of simultaneous multiple media stream decryption and encryption processing. The security processor includes a controller operative to be programmed through authenticated firmware downloads from a headend, each firmware download operative to modify media stream processing by the security processor. A memory stores the downloaded firmware. A plurality of digital stream encryption/decryption engines are selectively coupled by the controller for simultaneous operation in response to a predetermined security configuration downloaded to the controller.

As before, the Examiner relied on a combination of Pinder and Robbins to reject claim 20. The Examiner asserts that Pinder discloses that Appellants' "controller is operative to be programmed through download from a head-end, each download operative to modify media stream processing by the security processor (col. 25, lines 28-50; col. 26, lines 54-63; col. 29, etc.)" (Final Office Action, pg. 4.) The cited passages do not teach or fairly suggest

downloading programming into a controller. Rather, the passages disclose downloading encryption keys.

> Any one of the public keys for a CAA can be replaced by means of a sequence of two EMMs, the first of which has a sealed digest encrypted with the private key corresponding to a first one of the other two public keys, and the second of which has a sealed digest encrypted with the private key corresponding to the second one of the other two private keys. Each of the two EMMs contains an identifier, the CAAID for the new CAA, a key select value indicating which of the three CAA public keys is to be replaced, and the public key for the new CAA. After the first EMM is successfully authenticated by DHCTSE 627 by verifying the digital signature applied by the first CAA key, DHCTSE 627 computes a MD5 hash of the new CAA public key in this first EMM and stores it. After the second EMM is successfully authenticated by the DHCTSE by verifying the digital signature applied by the second CAA key, the DHCTSE computes a MD5 hash of the new CAA public key included in this second EMM. This second hash is compared with the first. If the hashes are identical, the new CAA public key and CAAID are substituted for the public key and CAAID of the CAA specified by the key select value. A single CAA public key must not be changed twice without one of the other two CAA public keys being changed in between.
>
> (Pinder, col. 25, ll. 28-50.)
>
> EMM header 1113 in all of these EMMs contains a CAAID for the CAA, and all of the EMMs have a sealed digest that has been encrypted with the CAA's private key. The CAA may use these EMMs not only to set up EA information 1333, but also to modify already existing EA information 1333 for an EA and to remove EA information 1333 for an EA. When the latter has been done, DHCTSE 627 will no longer respond to EMMs or ECMs from the entitlement agent.
>
> (Pinder, col. 26, ll. 54-63.)

The Examiner admits that Pinder "does not explicitly disclose wherein the downloads comprise firmware." (Final Office Action, pg. 4.) As argued above, Pinder not only fails to disclose firmware downloads, Pinder actively teaches away from Appellants'

"controller operative to be programmed through authenticated firmware downloads from a headend, each firmware download operative to modify media stream processing by the security processor" as in claim 20. (*See,* Pinder, col. 21, ln. 49-col. 22, ln. 12, quoted above.)

Once again, the Examiner relied on Robbins' disclosure at "col. 5, lines 1-6; col. 13, lines 65-67." (Final Office Action, pg. 4, cited text provided above.) As provided above, neither Robbins nor Pinder teach or fairly suggest the claimed firmware download. Moreover Pinder, the Examiner's primary reference, actively teaches away from any combination that might disclose Appellants' firmware download. Claim 20 is patentable over any combination of Pinder and Robbins. Claims 21-28, which depend from claim 20, are therefore also patentable.

3. Claim 22 Is Separately Patentable <u>Over Pinder In View Of Robbins</u>

Claim 22, which depends from claim 20, further provides that the security configuration downloaded to the controller comprises at least one of Data Encryption Standard (DES), Triple DES (3-DES), Advanced Encryption Standard (AES), and Common Scrambling Algorithm (CSA). The Examiner rejected claim 22 as disclosed by Pinder, providing as support only "col. 5, lines 10-15; col. 6, lines 45-50." (Final Office Action, pg. 5.) These passages, provided below, disclose the use of encryption techniques, not Appellants' configuration downloaded into the controller as claimed.

> The encryption and decryption techniques used for service instance encoding and decoding belong to two general classes: symmetrical key techniques and public key techniques. A symmetrical key encryption system is one in which each of the entities wishing to communicate has a copy of a key; the sending entity encrypts the message using its copy of the key and the receiving entity decrypts the message using its copy of the key. An example symmetrical key encryption-decryption system is the Digital Encryption Standard (DES) system. A public key encryption system is one in which each of the entities wishing to communicate has its own public key-private key pair. A message encrypted with the public key can only be decrypted with the

> private key and vice-versa. Thus, as long as a given entity keeps its private key secret, it can provide its public key to any other entity that wishes to communicate with it. The other entity simply encrypts the message it wishes to send to the given entity with the given entity's public key and the given entity uses its private key to decrypt the message. Where entities are exchanging messages using public key encryption, each entity must have the other's public key. The private key can also be used in digital signature operations, to provide authentication. For details on encryption generally and symmetrical key and public key encryption in particular, see Bruce Schneier, *Applied Cryptography*, John Wiley and Sons, New York, 1994.
>
> (Pinder, col. 5, ll. 5-30.)
>
> This encryption is preferably a symmetric cipher such as the Triple-DES algorithm using two distinct 56-bit keys (which taken together comprise MSK [Multi-Session key] 208).
>
> The MSK 208 has a longer lifetime than CW 202. The MSK lifetime is typically hours to days in length. MSK 208 is both encrypted and digitally signed by MSK Encrypt & Digital Signature function 206 before being sent to MUX 200 encapsulated in EMM 111.
>
> (Pinder, col. 6, ll. 45-52.)

The Examiner cannot help but admit that "the encryption algorithms may be hardcoded into the Pinder device." (Advisory Action, pg. 2.) As pointed out above, Pinder expressly states that the encryption algorithms are placed in memory "which is read-only memory whose contents are fixed when DHCTSE 627 is manufactured." (*See,* Pinder, col. 21, ln. 49-col. 22, ln. 12.) Thus, even if claim 20 is deemed to be unpatentable, claim 22 is patentable over the cited prior art.

4. **Claim 23 Is Separately Patentable <u>Over Pinder In View Of Robbins</u>**

Claim 23, which depends from claim 20, further provides that the security configuration downloaded to the controller comprises at least one of a secure download, RSA key management, multiple security key management, authentication, copy protection, and

digital signatures. The Examiner rejected claim 23 as disclosed by Pinder, providing as support only "col. 6, lines 50-65." (Final Office Action, pg. 5.) This passage, provided below, discloses the use of encryption techniques, not Appellants' configuration which is downloaded into the controller as claimed.

> The MSK 208 has a longer lifetime than CW 202. The MSK lifetime is typically hours to days in length. MSK 208 is both encrypted and digitally signed by MSK Encrypt & Digital Signature function 206 before being sent to MUX 200 encapsulated in EMM 111. MSK 208 and other parts of EMM 111 are preferably encrypted using a public key algorithm, such as the well-known RSA algorithm, with a public key associated with the specific set-top box 113 to which the EMM is addressed. The public keys of all set-top boxes 113 in a system 101 are stored in Public Key Data Base 207. The public keys in this data base are preferably certified by a certificate authority. The digital signature function in 206 is preferably the RSA digital signature method, although others could be used. In the case of an RSA digital signature, the private key which is used to make the signature belongs to the entitlement agent within service distribution organization 103 responsible for authorizing the associated service.
>
> (Pinder, col. 6, ll. 48-65.)

The Examiner cannot help but admit that "the encryption algorithms may be hardcoded into the Pinder device." (Advisory Action, pg. 2.) As pointed out above, Pinder expressly states that the encryption algorithms are placed in memory "which is read-only memory whose contents are fixed when DHCTSE 627 is manufactured." (*See,* Pinder, col. 21, ln. 49-col. 22, ln. 12.) Thus, even if claim 20 is deemed to be unpatentable, claim 23 is patentable over the cited prior art.

Please withdraw the fee of $510 as applicable under the provisions of 37 C.F.R. § 41.20(b)(2) from our Deposit Account No. 02-3978. Please charge any additional fee or credit any overpayment in connection with this filing to our Deposit Account No. 02-3978.

Respectfully submitted,

JAMES W. FAHRNY et al.

By: ______________________
Mark D. Chuey, Ph.D.
Registration No. 42,415
Attorney/Agent for Appellants

Date: December 11, 2007

BROOKS KUSHMAN P.C.
1000 Town Center, 22nd Floor
Southfield, MI 48075-1238
Phone: 248-358-4400
Fax: 248-358-3351

Enclosure - Appendices

VIII. CLAIMS APPENDIX

Claims 1-28, as provided below, are pending on appeal.

1. A system for multi-stream security processing and distributing digital media streams, the system comprising:

a headend configured to generate encrypted digital media streams and download software;

a network coupled to the headend and configured to receive the encrypted digital media streams and downloaded software; and

at least one receiver coupled to the network and configured to receive the encrypted digital media streams and downloaded software and to present a decrypted version of the encrypted digital media streams based on the downloaded software, wherein the receiver comprises a security processor configured to provide at least one of simultaneous multiple encryption and simultaneous multiple decryption processing of the digital media streams, the security processor operative to store the downloaded software and to securely configure, renew, and re-configure at least one of encryption and decryption by the security processor based on the downloaded software.

2. The system of claim 1 wherein the media streams are at least one of a video stream, and audio stream, and a video plus audio stream.

3. The system of claim 1 wherein the security processor comprises a plurality of digital stream encryption/decryption engines that are selectively parallel coupled by a controller for simultaneous operation in response to a predetermined security configuration.

4. The system of claim 3 wherein the security configuration comprises at least one of Data Encryption Standard (DES), Triple DES (3-DES), Advanced Encryption Standard (AES), and Common Scrambling Algorithm (CSA).

5. The system of claim 3 wherein the security configuration comprises at least one of a secure download, RSA key management, multiple security key management, authentication, copy protection, and digital signatures.

6. The system of claim 3 wherein the security processor further comprises at least one of a memory containing a hash, engine encryption/decryption configuration logic, a random number generator, a multiplier, and a memory containing a dynamic feedback arrangement scrambling technique (DFAST) algorithm coupled in parallel to the controller and configured to provide multiple key management for at least one of conditional access and digital rights management.

7. The system of claim 3 wherein the security processor further comprises at least one of a swappable random access memory (RAM) and a swappable flash memory containing the predetermined security configuration.

8. The system of claim 3 wherein the security processor provides role-based authentication that is used by an authorized user for at least one of configuration, reconfiguration, and renewal.

9. The system of claim 1, wherein the receiver is at least one of a set top box (STB), and a receiver or transceiver for at least one of digital televison, high definition digital television (HDTV), audio, MP3, text messaging, and game digital streams.

10. The system of claim 1, wherein the receiver is a set top box (STB) and the system further comprises an additional receiving device including the security processor, coupled to the STB and configured to receive and decrypt the encrypted digital media streams using the security processor.

11. A method of multi-stream security processing and distributing digital media streams, the method comprising:

generating encrypted digital media streams at a headend;

coupling a network to the headend and receiving the encrypted digital media streams at the network;

coupling a receiver to the network, the receiver receiving a software download from the network;

receiving the encrypted digital media streams at the receiver, and presenting a decrypted version of the encrypted digital media streams using the receiver;

re-configuring a security processor in the receiver based on the software download to provide at least one of simultaneous multiple encryption and simultaneous multiple decryption processing of the digital media streams; and

storing the software download in the security processor.

12. The method of claim 11 wherein the media streams are at least one of a video stream, and audio stream, and a video plus audio stream.

13. The method of claim 11 wherein the security processor comprises a plurality of digital stream encryption/decryption engines that are selectively coupled by a controller for simultaneous operation in response to a predetermined security configuration.

14. The method of claim 13 wherein the security configuration comprises at least one of Data Encryption Standard (DES), Triple DES (3-DES), Advanced Encryption Standard (AES), and Common Scrambling Algorithm (CSA).

15. The method of claim 13 wherein the security configuration comprises at least one of a secure download, RSA key management, multiple security key management, authentication, copy protection, and digital signatures.

16. The method of claim 13 wherein the security processor further comprises at least one of a memory containing a hash, engine encryption/decryption configuration logic, a random number generator, a multiplier, and a memory containing a dynamic feedback arrangement scrambling technique (DFAST) algorithm coupled to the controller and configured to provide multiple key management for at least one of conditional access and digital rights management.

17. The method of claim 13 wherein the security processor further comprises at least one of a swappable random access memory (RAM) and a swappable flash memory containing the predetermined security configuration.

18. The method of claim 11 further comprising:

presenting the encrypted digital media streams from the receiver; and

coupling an additional receiving device including the security processor to the receiver and receiving and decrypting the encrypted digital media streams at the receiving device using the security processor.

19. The method of claim 11 wherein the security processor provides role-based authentication that is used by an authorized user for at least one of configuration, reconfiguration, and renewal.

20. For use in a system for multi-stream security processing and distributing digital media streams, a security processor configured to provide at least one of simultaneous multiple media stream decryption and encryption processing, the security processor comprising:

a controller operative to be programmed through authenticated firmware downloads from a headend, each firmware download operative to modify media stream processing by the security processor;

a memory for storing the downloaded firmware; and

a plurality of digital stream encryption/decryption engines that are selectively coupled by the controller for simultaneous operation in response to a predetermined security configuration downloaded to the controller.

21. The security processor of claim 20 wherein the media streams are at least one of a video stream, and audio stream, and a video plus audio stream.

22. The security processor of claim 20 wherein the security configuration comprises at least one of Data Encryption Standard (DES), Triple DES (3-DES), Advanced Encryption Standard (AES), and Common Scrambling Algorithm (CSA).

23. The security processor of claim 20 wherein the security configuration comprises at least one of a secure download, RSA key management, multiple security key management, authentication, copy protection, and digital signatures.

24. The security processor of claim 20 wherein the security processor further comprises at least one of a memory containing a hash, engine encryption/decryption configuration logic, a random number generator, a multiplier, and a memory containing a dynamic feedback arrangement scrambling technique (DFAST) algorithm coupled to the controller and configured to provide multiple key management for at least one of conditional access and digital rights management.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.